International Journal of Science Academic Research
Vol. 03, Issue 11, pp.4676-4679, November, 2022
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

ENHANCING GLOBAL SECURITY AND PEACEFUL COEXISTENCE: THE IMPERATIVES OF CYBERSEURITY ARCHITECTURE

[1, *]Emmanuel Eturpa SALAMI and [2]Olusoji David POPOOLA

[1]Department of Computer Science, College of Natural and Applied Science, Igbinedion University Okada, Edo State, Nigeria
[2]Department of Sociology and Anthropology, College of Arts and Social Sciences, Igbinedion University Okada, Edo State, Nigeria

Received 12th September 2022; **Accepted** 19th October 2022; **Published online** 30th November 2022

Abstract

The greatest threat to world peace and security in recent times are those happening through the cyberspace. The sophistication and devastations of these threats recorded through cyberattacks across the world in recent times has brought to the fore the vulnerabilities of both strong and weak nations. Today warfare, whether political or economic between nations or states have metamorphosed from the conventional modes into a cyberwarfare which is more deadly and this has severely jeopardized global security and peace of humanity. This study examined how global security and peaceful coexistence can be enhanced through the sharpening of cybersecurity architecture. In the study, some incidences of cyberattacks across the world were examined, responses of the global community were reviewed, African nations experiences of cybersecurity threats were discussed among others. Standing on the game theory, (Non-zero Sum), the study suggested an integrated approach to formulating and implementing workable global cybersecurity architecture where the interests of all stakeholders are factored in and protected.

Keywords: Cybersecurity, Global Security, Peaceful coexistence.

INTRODUCTION

The security and peace of nations globally has come under severe threats as a result of the ever-increasing offensive attacks to both critical infrastructures and human privacy through the cyberspace. Cyberspace is a defining feature of modern life hence, Individuals and communities worldwide connect, socialize, and organize themselves in and through cyberspace. The existence of numerous cyber security issues on various spheres of life naturally increases political interest in resolving them. There isan ever-widening range of activities encompassing espionage, surveillance, privacy intrusions, denial-of-service attacks, ransom ware, and malware operations that has impacted nations and individuals negatively" (Freedom, 2019).These issues to a great extent affect the peace and security of nations globally therefore the need to review existing cybersecurity architecture is now very imperative. Cybersecurity was first seen as an international threat around 1990-1994, when a group of Dutch teenagers successfully hacked into U.S. military institutions prior to the First Gulf War and were able to gather information on missiles and nuclear weapons for over a year before they were being detected. If such attack had been carried out by people hostile to the U.S, it could have significantly changed the outcome of the war. In "Moonlight Maze", a 1998 incident, where an alleged Russian spies intruded on the U.S. military as well as some U.S. universities is another instance of cyberattack. The attack was traced to Russia, though that does not necessarily indicate the source of the attack. The U.S. called it a "state sponsored attack," and whether or not it was, this incident made the possibility of international, state-backed cyber-attacks a reality (Post, 2015). No nation in the world can claim immunity from these threats this was evident from the 911 attack by terrorist on United State of America in 2001 and its aftermath on world peace and security which has led to the ongoing crisis in countries such as Iran, Iraq and Yemen. The attack on the Irian nuclear power plant that has now led to Irian having to confront the Israeli nation as to authenticity of the attack being a cyberattack or not (Corera, 2021) is a case pointing to how national security can be threaten using the instrumentality of cyberattack. Aonther case in hand was the Russia-georgia war that started in July 2008 where Russia used "Zombie" computers to perform a Denial of Service (DoS) attack against the then Georgian president's website and also attack the OS Inform New Agency and OSIRadio. In Africa, cyber attacks have majorly been in the financial sector in 2020 as reported by africanews (Africanews, 2020) which means that the economy of african states will continue to experience crisis that can causea severeeffect on the security and peace of the states. There's indeed a nexus between political, socioeconmic stability and security of any nation therefore, it is imperative for nations and states to look at their existing cybersecurity architecture with a view to remodel it to address the myraids of contemporary problems that shall arise and will still arise in the near future as a result of cyberspace attack.

Corresponding Author:** ***Emmanuel Eturpa SALAMI
Department of Computer Science, College of Natural and Applied Science, Igbinedion University Okada, Edo State, Nigeria.

Theorctical Review

Consistent with the perspectives of the game theory, the study advocate a synergy between the "Strong" and "Weak" nations especially at evovling workable Cyberseucirty Architecture globally. The game theory involves the strategic decision making among sakeholders on critical issues that provides threats to them. (Wiiliams, 1993) described the perspectives of the game theory as one, which entails conflict and cooperation between intelligent, rational decision-makers. In other words, there are elements of conflict but yet the decision to cooperate may be chosen when rational and intelligent decision makers are involved. Critical to the game theory as the fact that the decision making process thrives in a situation where the outcome depend upon the choices made by one or more of

players. The term "game" was not used in the convectional sense but describes any situation involving positive or negative outcomes determined by the players choices and in some cases, chance. In this study for instance, the extent to which the global space is secured or vulnerable depends on the choices made by the stakeholders such as the United Nation Security Council, United States, and other critical stakeholders in world peace. The game theory is premised on some assumptions. For instance, it assume that each player is rational, each player is acting in self-interest and that players choices determine the outcome of the game but each palyer has only partial control of the outcome. The game theory was invented by a popular mathematician John Neuman and an Economist Oskar Mogensten (2007) reflected in their classical book called "Theory of games and economic behaviour". The theory made contributions in defining nuclear strategy and cybernetics. There are two sides to the game theory: the 'Zero Sum games' and the 'Non-Zero Sum game'. In the zero sum game, the gains of one person is exactly equal to the net losses of the other participant or participants. In other words, "the winner takes it all syndrome". The non-zero sum game is the opposite of the zero sum theor, it involves a situation that every stakeholder make contribution and shares in the benefits. The type that is releveant to the issue of cybersecurity and global peace is the non-zero sum game theory. The non-zero sum game theory emphaises no universal solution or a single optional strategy that is preferrable to all others nor is there a predictable outcome. It is also not strictly competetive as opposed to the zero sum game theory but the game in a non-zero sum generally have comptetive and cooperative elements. Players in a non-zero sum have some complementary interest and some interests that are completely opposed. Thus, one player's gain does not necessarily mean another players loss (and vice versal), as the gains and losses in the game do not make all sorts of degrees of cooperation and depending on how much cooperation is permitted in the game, the strategies of each player can change quite a bit. In this study therefore, stakeholders comes-in with various interests and positions, many of which may be opposing to each other. Non-zero Sum game theory expect that individual interest group will find a wa to accommodate other stakeholders interest in order to foster common Cybersecurity architecture that can serve the interests of all members and ensure global peace in this situation therefore all interest are considered, sacrifices and concerns are made, cooperation is ehanced and the overall goal is achieved.

Overview of Global Efforts on Cybersecurity

The United Nation Security council (UNSC) chief disarmament officer in his presentation on "Explosive Growth of Digital Technologies Creating New Potential for Conflict" which is the first ever debates on maintaining peace and security in cyberspace that was held in June 2021 identified key issues such as; how disinformation campaigns is affecting the disruption of computer networks and contributing to the diminishing trust and confidence among States. Particularly key areas observed to be at risk is critical infrastructures that includes financial institutions, health care facilities and energy grids since these infrastructures rely heavily on information and communications technology (ICT) to function. These indeed shows the growing concern for the need for awareness on the impact of cybersecurity to the world peace and security of humanity. Several charters and treaties have been drafted by the United Nation (UN) all to enhance security and peace. Today the greatest danger to the security of nations as observed by UN "does not lie at the crossroads of radicalism and technology but at the point where the urgency of a well-integrated common approach to tackle the problem and approach is being ignored but which must be done with the realities of today's security threats".

UN high level panel setup to study and report on emerging threats, challenges and changes, identified six areas of threats that will become serious threats in the future; (i) Internal conflict, including civil wars, genocide and other large-scale atrocities. (ii) Nuclear, radiological, chemical and biological weapons. (iii) Terrorism. (iv) Trans-national Organized crime. (v)Economic and social threat and (vi) Inter-state conflict. (Altes, 2006) critical to these threats is the medium through which such threats will be carried out, one of which is the cyberspace. The cyberspace today is an open channel for executing threats to global peace and security. Some states, and possibly as many as 30, are developing or have in place offensive cyber capabilities in connection with their military structures and/or doctrine. Some, including NATO, have acknowledged cyber space as a new operational domain of warfare (Freedom, 2019). There are various legal documents drafted to address issues of information security (cybersecurity) by UN, such as; "*The right to privacy as guaranteed by Article 17 of the International Covenant on Civil and Political Rights (1966). Article 15 of the International Covenant on Economic, Social and Cultural Rights (1966) protects the right of everyone to "enjoy the benefits of scientific progress and its applications" which can be interpreted to include the right to use the Internet"; "The right to privacy in the digital age has also been taken up by the UNGA Third Committee."* these are all aimed at ensuring global peace.

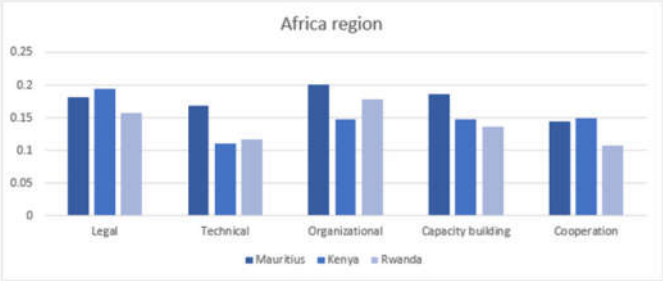
In an attempt to further ensure a global cyber hygiene which will promote global security and peace, more than 60 nations and 130 companies as well as 90 universities in Paris met in November 2018 to sign a document which is called 'Paris Call for Trust and Security in cyberspace' (Shackelford, 2019) this document broadly state principles that should be adopted in the security of digital products and services as well as integrity of the internet. Though the document does not bind any of the participant legally, it however provided some basic guides which can be adopted in enforcement of standards. Also, more recently in New Zealand governments of 18 nations met with tech giants like Google and Facebook to adopt a document called "Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online" all these efforts are toward promoting a secure and peaceful coexistence among nations especially with the regards to activities that goes on online. A new angle to enhancing global security and peace is the call to make cybersecurity a human right just as freedom of speech and expression are regarded as human right and this is hoped to make both governments and nations put in place a structured framework that will protect their citizens. The need for a review of existing global cybersecurity architecture is very imperative as this will help developing nations particularly to understand the ramification of it impact and how to manage the cybersecurity risk that might affect their critical infrastructures.

Cybersecurity Threats and Attacks in the Africa continent

Africa states are more prone to cyberattacks which might threaten their peace since most of their cybersecurity

framework and infrastructure are still below the minimum required standard. In the 1st and 2nd quarter of 2021 report from africanews.com (APO-Group, 2021)it shows that South Africa, Kenya and Nigeria experienced the highest cybersecurity attacks particularly in their financial sectors ranging from ransom ware (24%), crypto-miner malware (14%) and trojans (59%) attacks and since the financial sector of any nation to a large extend will affect their stability, this shows that if nothing is done to address the issue, it will have an impact on the peace of these nations. The outbreak of COVID-19 also has led to an upsurge in sophisticated phishing email schemes by cybercriminals where malicious actors are posing as the Center for Disease Control and Prevention (CDC) or World Health Organization (WHO) representatives and such attack to the health sector could lead to mass death. When the cybersecurity mitigation efforts of African nations were evaluated, five pillars used for measurement were used; the Legal efforts, Organizational efforts, Technical efforts, Capacity building and Cooperation efforts, it reveals that only few countries seem to be doing fairly well in addressing the issues. Kenya, Mauritius and Rwanda are leading in these five areas which shows again that a lot needs to be done by African government, IT experts and cooperation.

Table 1. Cybersecurity measurement pillars



(Source: ITU Publications)

African nations must awake to the urgency of addressing the problem of cybersecurity in the continent through collaborative effort and were possible, they can adopt a unified architectural framework that best suits the African states. There must be more awareness by organizations as well as government through policies on cybersecurity that reflect the prevailing security threats that are known and those yet to happen. The cybersecurity posture of most African countries makes the continent a soft target and an easy route for deploying an offensive attack against other nations. The existing policies within the continent are at best disjointed in the sense that attackers can easily invade punishment from one state by escaping into another without necessarily been caught because of lack of willingness of states to cooperate in establishing a single defensive frontier against cyberattacks.

Solutions to Cyber Insecurity

The war against cybersecurity can be mitigate or manage through a 'Tripartite Architectural cybersecurity approach' involving the International Communities, Government/States and Cooperation/Businesses. cybersecurity protection or defenseisa capital-intensive project and requires collaboration among nations. A well-structured policy that is implementable must be developed and central to such architectural design should be training and retraining of professionals in the field of cybersecurity defensive approach and awareness creation among citizens. The era of policy formulation that looks excellent in theory can no longer subsist today as seen in the cybersecurity architecture of some African states. Policy adoption from other nations or states should be done to reflect the current realities of each nation.

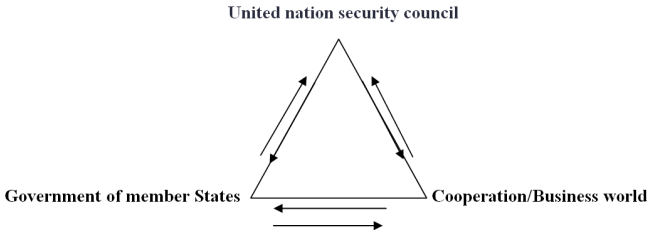


Figure 1. Cybersecurity Architecture Model

United Nation Security council: As the international coordinating organ comprising of regional cybersecurity professionals drawn both from the academia and industries need to harmonize existing cybersecurity policies (Laws, Regulations and Guides) from different regions in such a way that it will give all region advantage to benefit from the strengths of others and vice versal therefore making every region to be on the same standard applying the non-zero-sum game theory. The policies will ensure the states within the regional security organization understand the defensive methods as it is applicable to them. All policies develop should be one that can be easily implementable by States and Cooperation.

Government of member States: The political and nonpolitical actors within a nation who have the responsibility of drafting, designing and implementing policies should draft national cybersecurity laws to be in tandem with regional policies but putting into consideration the uniqueness of their regions.

Cooperation/Business world: national and local cooperation and businesses must as a matter of urgency show more wiliness to play a pivotal role in the training of their staffs on cybersecurity defensive approach as this will help save guard business critical infrastructure and integrating the culture of cybersecurity protective approach in the work place will better enhance the safety of business operations both at the international and regional level.

Conclusion

The reoccurring cases of states, government and cooperate sponsored attacks through cyberspace will only aggravate the insecurity already witnessed and losses recorded in time past if the global committee of nations don't act fast. Past incidences might just be 'a tip in the ice-burg' with many more waiting to happen. It is therefore very pertinent for the United Nation and other regional bodies concerned take a decisive step in reviewing the existing security architecture with a focus on cybersecurity as this has become a trending issue that will to a great extend affect global security and peace of many nations especially the developing countries that are still struggling to catch up with the ever-growing cybersecurity challenges globally. Adopting the Non-Zero-Sum game theory in enhancing global security and peace for coexisting will require more collective security work and this will include, finding a way to reduce the Weaponization of Space and an unequivocal international commitment to the exclusive peaceful use of Outer Space. As earlier identified, nations (developed and

developing) are all stakeholders as only collective efforts that can lessen the attacks. The humanitarian and human rights impact of cyber operations be a guiding principle and central to multilateral discussions of cyber peace and security rather than being treated as a secondary after-thought to national security concerns. The call for an international treaty for cyberspace that will clearly look into how humans can be protected from future cyber warfare is more urgent now than ever. African nations must wake up to the urgency of addressing the problem of cybersecurity in the continent through collaborative effort and were possible, the adoption of a unified architectural framework that best suits the African states should be considered. More awareness among the populace needs to be carried out starting from the primary, secondary to tertiary institutions so that the new generation of youth will be adequately informed to develop a positive mindset that will contribute to the peace of their regions and states. Both organizational and government policies on cybersecurity should reflect the prevailing security threats that are known and those yet to happen with the standardized approach in mitigating them.

REFERENCES

Altes, E. 2006. Reflections On Peace And Security In The 21st Century. Retrieved 09 27, 2021, from https://paricenter.com/library/economics-ethics-and-globalization/reflections-on-peace-and-security-in-the-21st-century/

APO-Group, 2021. Cyberattacks in Africa comparable to other parts of the globe, says Kaspersky. Africanews.

Brunot, R. 2018. *UNSC-Final.pdf.* Retrieved from Cleveland Council on world Affairs: https://www.ccwa.org/wp-content/uploads/2018/09/UNSC-Final.pdf

Corera, G. 2021. *World-middle-east-56722181*. Retrieved 10 1, 2021, from bbc.com: https://www.bbc.com/news/world-middle-east-56722181

Freedom, W. I. 2019. *Cyber peace and security.* Retrieved 09 28, 2021, from https://reachingcriticalwill.org: https://reachingcriticalwill.org/resources/fact-sheets/critical-issues/14010-cyber-peace-and-security

Neethling, T. 2005. Nexus and the Imperative of Peacebuilding with Special Reference to the African Context. *African Journal on Conflict Resolution, 1*. Retrieved 09 29, 2021, from https://www.accord.org.za/ajcr-issues/ the-security-development-nexus-and-the-imperative-of-peacebuilding-with-special-reference-to-the-african-context/

Neuman, J. and Mogensten, O. 2007. Theory of games and econnomic behaviour. *Journal of Social Sciences*.

Post, T. W. 2015. A history of internet security. The Washington Post. Washington.

Shackelford, S. 2019. In a world of cyber threats, the push for cyber peace is growing. Retrieved from finchen/shutter stock.com: https://theconversation.com/in-a-world-of-cyber-threats-the-push-for-cyber-peace-is-growing-119419

Wiiliams, P. 1993. Prisoners Dilema.

****